WHAT IS CLAIMED IS:

1. A computerized method for reducing the false alarm rate of network intrusion detection systems, comprising:

receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host;

identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host;

identifying the operating system type from the operating system fingerprint;

comparing the attack type to the operating system type; and

indicating whether the target host is vulnerable to the attack based on the comparison.

2. The computerized method of Claim 1, further comprising storing the operating system fingerprint of the target host in a storage location for a time period.

3. The computerized method of Claim 1, further comprising:

monitoring a dynamic configuration protocol server;

detecting that a lease issue has occurred for a new target host;

accessing a storage location;

determining whether an operating system fingerprint for the new target host already exists in the storage location; and

if the operating system fingerprint for the new target host does exist, then purging the existing operating system fingerprint for the new target host from the storage location.

4. The computerized method of Claim 1, further comprising:

monitoring a dynamic configuration protocol server;

detecting that a lease expire has occurred for an existing target host;

accessing a storage location;

determining whether an operating system fingerprint for the existing target host already exists in the storage location; and

if the operating system fingerprint for the existing target host does not exist, then disregarding the lease expire; and

if the operating system fingerprint for the existing target host does exist, then purging the existing operating system fingerprint for the existing target host from the storage location.

5. The computerized method of Claim 1, further comprising:

after receiving the data packets, determining whether a format for the alarm is valid; and

if the format is not valid, then disregarding the alarm; otherwise

if the format is valid, then continuing the computerized method with the identifying characteristics step.

6. The computerized method of Claim 1, further comprising automatically alerting a network administrator if the target host is vulnerable to the attack.

7. A system for reducing the false alarm rate of network intrusion detection systems, comprising:

a network intrusion detection system operable to transmit one or more data packets associated with an alarm indicative of a potential attack on a target host;

a software program embodied in a computer readable medium, the software program, when executed by a processor, operable to:

receive the one or more data packets;

identify characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host;

identify the operating system type from the operating system fingerprint;

compare the attack type to the operating system type; and

indicate whether the target host is vulnerable to the attack based on the comparison.

7. The system of Claim 6, further comprising a storage location operable to store the operating system fingerprint of the target host for a time period.

9. The system of Claim 7, wherein the software program is further operable to:

monitor a dynamic configuration protocol server;

detect that a lease issue has occurred for a new target host;

access a storage location;

determine whether an operating system fingerprint for the new target host already exists in the storage location; and

if the operating system fingerprint for the new target host does exist, then the software program is further operable to purge the existing operating system fingerprint for the new target host from the storage location.

10. The system of Claim 7, wherein the software program is further operable to:

monitor a dynamic configuration protocol server;

detect that a lease expire has occurred for an existing target host;

access a storage location;

determine whether an operating system fingerprint for the existing target host already exists in the storage location; and

if the operating system fingerprint for the existing target host does not exist, then disregard the lease expire; and

if the operating system fingerprint for the existing target host does exist, then purge the existing operating system fingerprint for the existing target host from the storage location.

11. The system of Claim 7, wherein the software program is further operable to automatically alert a network administrator of the attack if the target host is vulnerable to the attack.

12. The system of Claim 7, wherein the software program has no knowledge of the protected network architecture.

13. The system of Claim 7, wherein the software program has no access to the protected network.

14. The system of Claim 7, wherein the NIDS is vendor independent.

15. The system of Claim 7, wherein the NIDS does not support passive operating system fingerprinting.

16. A system for reducing the false alarm rate of network intrusion detection systems, comprising:

means for receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host;

means for identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host;

means for identifying the operating system type from the operating system fingerprint;

means for comparing the attack type to the operating system type; and

means for indicating whether the target host is vulnerable to the attack based on the comparison.

17. The system of Claim 16, further comprising means for storing the operating system fingerprint of the target host for a time period.

18. The system of Claim 16, further comprising:

means for monitoring a dynamic configuration protocol server;

means for detecting that a lease issue has occurred for a new target host;

means for accessing a storage location;

means for determining whether an operating system fingerprint for the new target host already exists in the storage location; and

if the operating system fingerprint for the new target host does exist, then means for purging the

existing operating system fingerprint for the new target host from the storage location.

19. The system of Claim 16, further comprising:

means for monitoring a dynamic configuration protocol server;

means for detecting that a lease expire has occurred for an existing target host;

means for accessing a storage location;

means for determining whether an operating system fingerprint for the existing target host already exists in the storage location; and

if the operating system fingerprint for the existing target host does not exist, then means for disregarding the lease expire; and

if the operating system fingerprint for the existing target host does exist, then means for purging the existing operating system fingerprint for the existing target host from the storage location.

20. The system of Claim 16, further comprising:

after receiving the data packets, means for determining whether a format for the alarm is valid; and

if the format is not valid, then means for disregarding the alarm.

21. The system of Claim 16, further comprising means for automatically alerting a network administrator if the target host is vulnerable to the attack.